AIR WAR COLLEGE

AIR UNIVERSITY

CYBERWAR: ARE CIVILIANS BACK ON THE BATTLEFIELD

by

Patrick W. Franzese, Colonel, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Kimberly A. Hudson, PhD

17 February 2015

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
17 FEB 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyberwar: Are Civilians Back On The Battlefield	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air War College, Air University,,Maxwell AFB,,AL**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The growth of cyberspace is posing challenges to many aspects of the international system and foremost among them is the current Law of Armed Conflict (LOAC) paradigm. While humanitarian concerns have strongly influenced recent LOAC development, state interests???and not humanitarian concerns???ultimately determine how states conduct war. Accordingly, states will continually explore and consider the nascent opportunities presented by cyberspace to determine whether cyberspace operations enables them to more easily or efficiently achieve their political objectives. In doing so, state practice will challenge many of the current LOAC provisions.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**28**	

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Colonel Patrick W. Franzese is assigned to the Air War College, Air University, Maxwell AFB, Alabama. Prior to entering active duty, he attended Washington University in St. Louis, MO on a 4-year AFROTC scholarship. On 14 May 1993, Colonel Franzese graduated from Washington University and was commissioned a Second Lieutenant in the United States Air Force. He then entered the educational delay program and pursued his law degree at the University of Minnesota Law School. He graduated *cum laude* in May 1996 and was admitted to the Minnesota State Bar in October 1996. Since then, he has served as a Judge Advocate General and has held various positions to include a Staff Judge Advocate, Circuit Trial Counsel, Area Defense Counsel and Chief, Operations Law for USSTRATCOM. Colonel Franzese has also deployed as a member of the Combat Operations Division, Combined Air and Space Operations Center, Al Udeid AB, Qatar.

Abstract

The growth of cyberspace is posing challenges to many aspects of the international system and foremost among them is the current Law of Armed Conflict (LOAC) paradigm. While humanitarian concerns have strongly influenced recent LOAC development, state interests—and not humanitarian concerns—ultimately determine how states conduct war. Accordingly, states will continually explore and consider the nascent opportunities presented by cyberspace to determine whether cyberspace operations enables them to more easily or efficiently achieve their political objectives. In doing so, state practice will challenge many of the current LOAC provisions. Chief among these are rules regarding combatantcy and targeting of civilians. The rules concerning combatantcy developed because the state controlled a monopoly on the use of force and could only employ this force effectively through an organized military structure. However, the unique aspects of cyberspace challenges both the monopoly states have on the use of force and the need to employ that force through an organized military structure. Similarly, the rules concerning the targeting of civilians developed after states concluded that targeting civilians did not ultimately further their political objectives However, cyberspace provide states the opportunity to target civilians in a more efficient and less directly violent manner.

Introduction

The growing importance of cyberspace is unquestionable and affects nearly every facet of our lives. Its impact on the nation state, international relationships and world order is still evolving with many varying degrees of prognostications as to its ultimate effect. Some see the emergence of a "Cybered Westphalian Age" while others see cyberspace as diffusing power to non-state actors.[1] Similarly, the effect of cyberspace on how states will conduct military operations and fight wars is also subject to great debate and uncertainty. Some argue that it will fundamentally alter how war is fought while others see it as mostly a joint force enabler that does not modify the nature of war.[2]

As the importance of cyberspace and cyber operations have increased, so have the attempts to place them within the current Law of Armed Conflict (LOAC) paradigm. Most notable is the Tallinn Manual on the International Law Applicable to Cyber Warfare. These efforts provide valuable insight into how the current LOAC paradigm generally applies, or should apply, to military cyber operations. However, these efforts also acknowledge that cyberspace provide unique challenges and thus there is significant uncertainty as to how it specifically applies in various situations due to the lack of treaties, state practice or official public statements on military cyber operations.[3]

While the efforts to define how the current LOAC paradigm applies to military operations in cyberspace is important, they often overlook the more fundamental fact that cyberspace will alter the ways states fight wars and, as a result, will threaten the current LOAC paradigm. Since a full assessment of that subject far exceeds what can be addressed here, this paper will instead narrowly focus on the potential impact cyberspace may have on the rules regarding both combatancy and targeting civilians. This paper is broken down into three

sections. First, we will briefly look at the factors that drive the LOAC development with focus on why cyberspace will challenge the current paradigm. Second, we will look at the factors that drove combatant status development under LOAC and how the unique characteristics of cyberspace challenge this foundation. Finally, we will look at how the protection of civilian developed under LOAC and how cyberspace could weaken this protection.

LOAC Background

Since war began, people have attempted to define the proper limitations, if any, on its conduct. Scholars from ancient Hindu, Chinese, Greek and Babylonian civilizations as well as Christian writers have attempted to address questions such as what can be targeted, who can be killed, and what weapons can be used.[4] Overtime a school of thought based upon Christian ideals, commonly known as *just war* theory or tradition, developed and provided guidance as to how to both engage in war and conduct war. However, it was not until the Lieber Code was published in 1863 that we see "the first instance in western history in which the government of a sovereign nation established formal guidelines for its army's conduct toward its enemies." Since then, LOAC has continued to develop with each generation often providing different answers to similar situations. For example, the strategic bombing campaigns that indiscriminately targeted cities during World War II would unquestionably violate LOAC today.[5]

A central question is what accounts for these changes. Commentators have noted that in recent history, "LOAC has been largely driven by humanitarian concerns."[6] However, that observation begs a number of questions such as: Are recent generations more moral? Is warfare today less violent? Are human passions more subdued? One only has to scan the news headlines to realize that the answer is "no"; human nature has not changed and the nature of war has not changed. Instead, changes in LOAC reflect the fact state interests have changed. As

Clausewitz observed, "war is not merely an act of policy but a true political instrument, a continuation of political intercourse, carried on with other means."[7] Accordingly, not only are the decisions to engage in war driven by political considerations but so are the way a nation fights its wars. Thus, LOAC has been largely driven humanitarian concerns recently because states believe that it is in their best interests to fight war with those humanitarian interests in mind. Put succinctly by Telford Taylor, a prosecutor at Nuremburg, "[t]he laws of war as we know them today are not so much the product of cerebration as of changing conditions that made them appear desirable to rulers, statesman and generals alike."[8]

This statement is especially poignant since it underscores there is a utilitarian aspect of LOAC. Specifically, complying with LOAC does not inhibit a state from achieving its political objectives. Instead, complying with LOAC facilitates the achievement of a state's political objectives that commonly include both winning of the war and restoring the peace. Two examples evidence this point. First, consider humane treatment of prisoners of war. Defeating the adversaries fielded forces is the overriding objective in most conflicts, and "forcing the surrender of fielded forces is the most economical and rapid means of removing enemy troops from the field without paying a corresponding toll in friendly casualties."[9] To that end, history has demonstrated that humanely treating prisoners of war will entice enemy combatants to surrender thus furthering the political objective of winning the war. During WWII, for example, millions of German soldier surrendered, however, only 12,194 Japanese soldiers surrendered "because of indoctrination by the Japanese military and expectations of mistreatment after capture."[10] As a result, some of the most violent and bloody battles of WWII took place in the Pacific. More recently, in Gulf War I, Iraqi soldiers surrendered in mass numbers after being barraged with pamphlets promising humane treatment.[11] The humane treatment of Iraqi POWs

was later cited by a US General as a reason for believing that Iraqi soldiers would also surrender during Operation Iraqi Freedom.[12] Thus, when considering the mistreatment of POWs at Abu Ghraib the harm was not only the immediate harm to the POWs but also the long-term harm to the US military operations. As eloquently stated in a NY Times op-ed:

> Would it have been different if the perception of us as purveyors of torture and humiliation existed back then? Would tens of thousands of Iraqis have put down their weapons if they believed they were going to be humiliated, abused or tortured, or would they have fought? Had they chosen to fight, the war would have lasted longer and cost more and casualties would have skyrocketed. Our reputation in 1991 as the good guys paid dividends and supported our national interests. We must regain that reputation.[13]

A second example of the utilitarian nature of LOAC is the prohibitions of targeting civilians. History as demonstrated that targeting civilian populations inhibits the political objective of restoring long-term peace. Many tensions that exist today such as those in the Balkans or between Japan and China are traced to the inhumane treatment of a civilian population during conflict. As stated by Charles Francis Adams, great grandson of President John Adams, during an address at a meeting honoring Robert E. Lee,

> "…looking back over the awful past, replete with man's inhumanity to man, I insist that the verdict of history is distinct. That war is Hell at best, then make it Hell indeed, that cry is not original with us: far from it; it echoes down the ages…What was the result? Hell was indeed let loose; but so was Hate. Was the war made shorter? No! Not by an hour! It was simply made needlessly bitter, brutal and barbarous…"[14]

As LOAC is the outgrowth of states pursuing their political objectives and is utilitarian in nature, it follows that technological advances will significantly influence LOAC. First, technological advances present states with opportunities to conduct military operations in a new way. Improved transport from roads and trains, for example, both permitted military forces to have consistent supplies—thus preventing the need to live off the land and plunder—and allowed military forces to more easily keep prisoners.[15] Second, technological advances present states

with opportunities to conduct new types of military operations. For example, the advent of airpower increased the range and potential targets for a state's military forces, presenting states with both new means of achieving current political objectives and the possibility of achieving new political objectives. In sum, technological advances have repeatedly spurred on LOAC development and change as it presents states with new situations and opportunities to achieve its political objectives. Accordingly, the growth of cyberspace will cause states to reassess how it can achieve their political objectives and whether new political objectives are now feasible. This in turn will challenge the current LOAC paradigm as states begin to contemplate, develop and execute cyber operations in an attempt to realize these political objectives.

Combatant Status

Under LOAC, it is important to determine combatant status for two main reasons. First and foremost, a combatant is considered a lawful target and thus may be targeted at any time, whether on or off the battlefield, unless *hors de combat* (i.e., out of the fight due to surrendering or being sick, injured or wounded and thus unable to defend oneself).[16] Conversely, a noncombatant cannot be lawfully targeted.[17] Second, a combatant is entitled to prisoner of war status if captured.[18] Conversely, an unlawful combatant (i.e., a noncombatant who engages in conflict) is not entitled to prisoner of war status and may be tried by a civilian court for any crimes such as killing an enemy soldier.[19]

Distinguishing between what constitutes a combatant and a noncombatant, as well as determining who is entitled to the various protections and privileges, is seemingly easy on its face. The Lieber Code plainly stated, "[a]ll enemies in regular war are divided into two general classes--that is to say, into combatants and noncombatants, or unarmed citizens of the hostile government."[20] However, the Lieber code further acknowledged there were many gradations

among these two classes as it further noted that those individuals entitled to prisoner of war status were simply not soldiers, but also those "attached to the hostile enemy for active aid," "all those who are attached to the Army for its efficiency and promote directly to the object of the war," and "citizens who accompany an army for whatever purpose, such as salters, editors, or reporters of journals, or contractors."[21]

Since the Liber Code, LOAC continued to develop with the seemingly straightforward requirement that to be a lawful combatant an individual must be a member "of armed forces of a Party to the conflict."[22] Additionally, many experts further believe that to be considered a lawful combatant an individual must also (1) be commanded by a person responsible for his subordinates; (2) have a fixed distinctive emblem recognizable at a distance; (3) carry arms openly; and (4) conduct operations in accordance with the laws and customs of war.[23] However, as with the Lieber Code, combatant status and rights determination is much more complicated then these rules imply. Today, LOAC scholars refer to over twenty categories, statuses and terms when discussing combatancy.[24]

In order to understand how/why these rules developed, it is important to understand the context under which states created these rules. Specifically, the state has traditionally held a virtual monopoly on the employment of force and force was employed through an organized military. Accordingly, LOAC reflected that an individual who employed force was going to be a member of the armed forces, be commanded by a person responsible for his subordinates, have a fixed distinctive emblem recognizable at a distance and carry arms openly. However, as context changes—meaning that a state loses its monopoly on employing force and states acquire means to employ force other than through an organized military—so will the rules pertaining to combatant status and privileges.[25]

The continued growth of cyberspace and nascent opportunities presented by cyber operations will challenge the current LOAC paradigm because the five key characteristics on which the current combatancy rules were developed do not account for cyberspace's unique attributes. First, individuals who engaged in traditional warfare needed to be physically present on the battlefield. Throughout most of history, the means of fighting consisted mainly of individual weapons such as swords, spears, and bows that had limited range. Thus, war was essentially a mass of individuals engaging in hand-to-hand combat. With the advent of artillery, and increasing range of that artillery, an individual could be further removed from the battlefield and still engage in combat. Similarly, with the introduction of the airplane individuals did not need to be physically present on the battlefield although they nonetheless were in the airspace over it.

Cyberspace, however, breaks the physical nexus between the location of the individual who engages in military operations is located and the location of the target. Computer technology in the form of ballistic missiles, remotely piloted aircraft and robotics allow an individual to be far removed from the battlefield.[26] However, cyberspace operations take this one-step further by erasing any requirement for physical presence—through either an individual or machine/weapon—on the battlefield. The corresponding effect is that whereas traditional means of fighting war easily permit a state to identify the source of the attack (i.e., who launched the artillery, aircraft or missile), it is exceptionally difficult to attribute action in cyberspace.[27] Moreover, the removal of, or attempt to remove, individuals from the battlefield has had the paradoxical effect of actually expanding the battlefield as more legitimate targets are created and the demarcation between civilian and military becomes further obfuscated.

Second, individuals who engaged in traditional warfare needed specialized equipment. Since the technological means of fighting for most of history consisted mainly of individual weapons, an individual could personally acquire, if not build, the weapons with which they fought even if the state ultimately provided them. However, as military technology progressed, the weapons quickly exceeded the ability of a single individual to acquire or build. Modern weapons such as tanks, airplanes or artillery that have been the staple of a modern military for nearly a century are well beyond the means of individuals to personally build or procure.

Conversely, individuals who engage in cyber operations do not require specialized equipment. All that an individual requires, from a technological standpoint, is a computer and internet access; something that are increasingly within the means of any individual to acquire. Moreover, an individual using a computer has the ability to inflict wider, and more significant, harm than an individual using a sword or rifle or even employing a fighter jet, tank or artillery.

Third, individuals who engaged in traditional warfare needed specialized training. Even though warfare historically consisted of individuals engaging in hand-to-hand combat, armies still needed to learn small unit tactics and work as a cohesive unit to employ force effectively. With advanced weaponry, even more specialized training is required. The skills needed to fly a fighter jet, operate a tank or launch a missile can only be developed via military training due both to cost associated with acquiring the underlying weapons system and the cost with the training itself. For example, it costs approximately $2.6 million to train a fighter pilot.[28] Moreover, even today with advance weaponry, it is still crucial that militaries train both as a unit and in joint warfare.

Comparatively, individuals who engage in cyber operations do not require specialized military training. This is not to say that significant skill is not required in conducting cyber

operations. For example, being able to target a nuclear power plant would require not only computer skills but also technical knowledge of how a nuclear power plant operates generally and the targeted nuclear power plant operates specifically. Rather, an individual who engages in cyber operations does not require organized training or training as a unit. Moreover, since no specialized equipment is required, individuals possess the means to train themselves as hacking information and hacking tools are readily available on the internet. Additionally, to the extent that specialized training is required, the civilian sector is able to provide that training. In fact, "[t]he cyberwarfare mission is unique, many experts say, in that reservists bring training and expertize from their work in the civilian sector that can be far more advanced than what's found in the military itself."[29]

Fourth, the skills needed to fight traditional wars were not easily transferable to civilian society. An individual who developed traditional warfighting skills could not employ those skills for something other than combat. Essentially the individual could either fight for their home country or fight as a mercenary for another country. This trend has continued in modern times with a growth of private military companies who hire individuals with military backgrounds and provide services such as "combat operations, strategic planning, intelligence, risk assessment, operational support, training and technical skills."[30] Even then, however, there is limited opportunity to pursue these activities and even less opportunity to employ weapons systems such as a fighter aircraft, tanks or artillery. As a result, the state has not needed to compete with civilian society to retain those individuals who possess specialized war fighting skills and thus are be able to retain individuals who are the premier experts in those areas.

Comparatively, the skills needed to engage in cyber operations are easily transferable to civilian society. As a result, the state is forced to compete to retain the best talent due to the high

demand for computer skills in civilian society and, by some accounts, the military is losing the best talent. A recent Military Times headlines clearly captures this point when stating "In Supersecret Cyberwar Game, Civilian-Sector Techies Pummel Active-Duty Cyberwarriors."[31] Granted, these "civilian-sector techies" were reservists, but there likely has never been an equivalent headline boasting how civilian/reserves pilots or tank commanders "pummeled" their active duty counterparts.

Finally, in traditional warfare militaries dealt exclusively with employing force and there was little debate as to what constituted "force" or an "act of war." When militaries fought, the intent and result was physical harm and destruction to the opposing side. Thus, initially, a combatant could easily be identified as an individual who employed force. Then, as military operations became more complex and the need for, and importance of, logistics grew, the understanding of what constituted a combatant also expanded to include not only those who actually employed force but those who supported those operations. Conversely, there is no agreed upon definition of what exactly constitutes "use of force" in cyberspace and proposed frameworks, such as the one proffered in the Tallinn manual, will require the subjective assessment of a number of factors.[32] Thus, with no clear demarcation, states have greater latitude to use individuals who are not members of their armed forces when conducting cyber operations that further political objectives.

Taken together, the unique attributes of cyberspace weakens the monopoly states have held on employing force and provides states the means to employ force other than through an organized military. Individuals do not need to be trained by, or part of, an organized military to conduct cyber operations and they can conduct these cyber operations from virtually any location on Earth against any location on Earth. Civilians will be free to conduct operations without the

consent or involvement of the state of which they are a citizen and, as evidenced by such groups as Anonymous, civilians will form organizations that comprise people from various states. As important, states will likely need to rely on civilians for expertise when conducting operations and may want to rely on the civilians to conduct operations in order to leverage some of the unique aspects of cyberspace such as difficulty in attribution. States may alter organizational structures of their militaries, redefining what it means to be a member of the armed forces and exploring whether cyber operations are best executed by either contracting out certain operations or by simply sending out a call for volunteers to conduct operations against a certain objective. In sum, cyberspace weakens the foundation upon which states designed the rules regarding combatant status. As a result, the current LOAC paradigm will need to change to incorporate this new reality.

Targeting Civilians

For much of recorded history, there were little, if any, protections for civilians during war.[33] However, a consistent theme during the recent growth of LOAC is the attempt to shield civilians from war. This development was captured by the Lieber Code which stated that while civilians of the state at war were "subjected to the hardships of the war", that "[t]he principle has been more and more acknowledged that the unarmed citizen is to be spared in person, property, and honor as much as the exigencies of war will admit."[34] This concept was advanced further in the 1899 and 1907 Hague Conventions through provisions that required the "lives of persons…be respected" and prohibited the bombardment of undefended cities.[35] These rather modest provisions were greatly expanded in the 1949 thru Geneva Convention IV, which provided detailed protection to civilians during war.[36] However, it was not until 1977 that Protocol I to the Geneva Convention firmly established the principle of distinction in

international law by clearing stating that "[t]he civilian population as such, as well as individual civilians, shall not be the object of attack."[37]

Notably, however, the principle of distinction does not mean that a state may never harm a civilian during war under any conditions. Rather, a state may still harm a civilian as long as a state is directly targeting a valid military target and the corresponding harm to civilians or civilian objects is not "excessive in relation to the concrete and direct military advantage anticipated."[38] When considering the rules of distinction and proportionality together, we see that while the principle of distinction is consistent with the humanitarian emphasis in the recent development of LOAC the principle of proportionality ensures that the state is not overly restricted or otherwise prevented from employing force to pursue its interest even if civilians are killed.

The sad irony is that despite the developments in LOAC designed to protect civilians from being targeted directly "wars of the twentieth century turned out to be ever more hostile to those who were *not* doing the fighting."[39] (emphasis in original). In fact:

> [a]t the outset of the twentieth century, the number of civilians killed in war was low relative to the number of soldiers killed: one civilian per every eight soldiers. By the end of the century, the ratio had been reversed: now eight *civilians* get killed for every solider that falls in battle."[40] (emphasis in original)

This reversal is likely attributed to the fact that at the beginning of the twentieth century nation state war involving large armies dominated whereas by the end of the century ethnic based civil war and insurgencies involving civilian populations dominated. Nonetheless, this fact evidences that, despite existing "protections" under LOAC, civilians will be targeted if a party to the conflict believes doing so will further its political objectives.

This reality is further evidenced when observing the way LOAC developed during the advent and maturation of airpower, a promising technology that similar to cyberspace today

offered states unique opportunities when first introduced. The quest for manned flight started long before the Wright brothers finally achieved it in 1903. States, having experienced balloons and anticipating the advent of other forms of flight, agreed in the 1899 Hague Convention to "prohibit, for a term of five years, the launching of projectiles and explosives from balloons, or by other new methods of similar nature."[41] This treaty was renewed again in 1907 for a period extending to the close of the next peace conference.[42] This conference was initially scheduled for 1914, but then rescheduled for 1915 and ultimately cancelled due to World War I. Additionally, another Hague Convention that dealt with war on land specifically stated, "[t]he attack or bombardment, by whatever means, of towns, villages, dwellings, or buildings which are undefended is prohibited."[43] However, heading into WWI many acknowledged that bombing of cities would be legal and, to the extent any prohibition was in effect, states fighting in WWI largely ignored it and bombed cities, albeit ineffectively, both as a means of targeting morale and reprisal.[44]

The airpower lessons from WWI were inconclusive but some states believed that aerial bombing did undermine the will of the people and that long-range bombing could have significant impact in war since "modern industrial nations had exploitable weaknesses and vulnerabilities."[45] This belief was fostered by early airpower advocates such as Giulio Douhet who professed "[t]here will be no distinction any longer between soldiers and civilians" and that "[b]y bombing the most vital civilian centers it could spread terror through the nation and quickly break down [the state's] material and moral resistance."[46] The potential promises of airpower, however, were tempered by humanitarian concerns as seen in the Hague Rules of Air Warfare that were drafted in 1923. Specifically, the draft rules stated "[t]he use of tracer, incendiary, or explosive projectiles by or against aircraft is not prohibited," but further stated

"[a]erial bombardment for the purpose of terrorizing the civilian population, of destroying or damaging private property not of a military character, or of injuring noncombatants is prohibited."[47]

While these rules were not adopted, the major powers all declared at the beginning of WWII that bombing civilian targets was illegal and/or civilian populations would be spared.[48] However, the reality was that "strategic" bombing campaigns—that included the indiscriminate bombing of cities—played a large role in WWII.[49] A driving factor behind this approach was the belief that attacking the civilian morale in the case of Germany and civilians themselves in the case of Japan was a prerequisite for winning the war.[50] Unlike WWI, however, the lesson from WWII was that aerial bombardment did not achieve these goals. While civilians suffered greatly and died in larger number than Allied military casualties, their torment did not result in the collapse of the government(s) and did not end the war quicker.[51]

In short, the advent of airpower presented states with a new means of conducting military operations. The first inclination was to limit its use in war to existing paradigms. However, as the technology advanced, states searched for ways to use airpower to achieve their political objectives. While states voiced humanitarian concerns, they nonetheless targeted civilians as a means of coercing the opposing state. Then, only after it proved an ineffective means of achieving political objectives did states agree to LOAC provisions prohibiting it.

Similarly, cyberspace once again presents states with a news means of conducting military operations. The first inclination as evidenced by numerous books and articles is to fit this new means of warfare into the current LOAC paradigm. However, the mostly unstated reality is that cyberspace presents states with new options to achieve political objectives that once again involve civilian targets.

As stated earlier, the growing importance of cyberspace is unquestionable and affects nearly every facet of our lives. Moreover, nations increasingly depend upon cyberspace to operate its critical infrastructure. Stock markets, electric power grids, banking systems, food delivery systems and mass transit are but a few examples. Such reliance, however, has created vulnerabilities and states are exploring them. Recently, for example, the Director of the National Security Agency told Congress that China as well as "one or two" other actors could shut down parts of the nation's electric grid via a cyberattack and that "adversaries are performing electronic 'reconnaissance' on a regular basis so that they can be in a position to attack the industrial control systems that run everything from chemical facilities to water treatment plants."[52] Notably, experts say the US also possesses this capability.[53]

While some of this critical infrastructure likely has a direct military nexus (e.g., the electrical grid that supplies power to a military installation), much of this critical infrastructure does not. Thus, the "reconnaissance" conducted by states signals that states are, at the very least, exploring the feasibility of targeting civilian objects. In other words, we are possibly seeing a re-birth of Douhet's strategy of attacking the morale of the people only this time via cyberspace. Whereas early airpower advocates believed that states could be coerced through bombing civilians, advocates of cyberspace operations are likely to argue that states can be coerced through either the direct harm (e.g., causing a dam to release water or causing a nuclear power plant to release radiation) or indirect social chaos (e.g., wiping out banking information or crashing communications needed for food delivery) that would, or could, ensue after a successful cyber operation against a state's critical infrastructure.

In sum, to the extent LOAC ever protected civilians, cyberspace weakens this protection. Cyberspace presents states, and non-state actors, intriguing opportunities to achieve political

objectives and they are exploring them. Not only will civilian targets once again be contemplated, but what it means to target civilians and civilian objects will also be further questioned. The current LOAC paradigm that ultimately aims to protect civilians is not adequate to deal with cyberspace.

Conclusion

Cyberspace has truly revolutionized the world. The way we interact, work and conduct our daily lives today was the fantasy of science fiction writers twenty-five years ago. Many commentators reflect that this revolution has made the world smaller. Paradoxically, however, it has expanded the potential battlefield. Not only will cyberspace require states to look at different ways to employ force and conduct coercive operations, but states will also consider a larger target set. While the humanitarian concerns underlying LOAC are noble and something to aspire to, we must ultimately deal with the world that way it is and not the way we wish it were. Throughout history, states have shown that they will pursue their political objectives through any means available. Thus, while humanitarian concerns have been increasingly important, those concerns are ultimately subordinate to the achievement of political objectives. In other words, LOAC is not a suicide pact. Hopefully, states will determine that humanitarian concerns continue to facilitate achievement of their political objectives. Nonetheless, the opportunities presented by cyberspace will entice states to act in a way that threatens the current LOAC paradigm and once again bring civilians back on the battlefield.

Notes

[1]*See generally* Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly*, Spring 2011, 32-61; Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), 113-151.

[2] *See generally* Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010); Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College Press, 2013).

[3] *See generally* Michael N. Schmitt, ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

[4]Leon Friedman, ed., *The Law of War: A Documentary History.* Vol. I. II vols (New York: Random House, 1972), 1-15.

[5]Ingrid Detter, *The Law of War, second edition* (New York: Cambridge Universty Press, 2000), 284-285; Gary D. Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (New York: Cambridge University Press, 2010), 80, 256-257.

[6] Solis, *The Law of Armed Conflict*, 7.

[7] Carl von Clausewitz, *On War*, ed and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 87.

[8]Friedman, *The Law of War*, xiii.

[9] Paul J. Springer, *America's Captives: Treatment of POWs from the Revolutionary War to the War on Terror* (Lawrence: University of Kansas Press, 2010), 3.

[10] Springer, *America's Captives*, 149

[11] SGM (Ret.) Herbert A. Friedman, *Leaflets of Operation Desert Shield and Desert Storm (continued).* http://www.psywarrior.com/HerbDStorm2.html (accessed 17 November 2014); Department of Defense, *Conduct of the Persian Gulf War: Final Report to Congress*, http://www.dod.mil/pubs/foi/operation_and_plans/PersianGulfWar/404.pdf, April 1992 (accessed 17 November 2014).

[12] Andrea Gerlin and Patrick Peterson, *philly.com,* March 13, 2003, http://articles.philly.com/2003-03-13/news/25474267_1_chemical-warfare-iraqi-soldiers-iraq-kuwait (accessed 17 Novmeber 2014).

[13] Morris Davis, "Unforgivable Behavior, Inadmissible Evidence (Op-ed)," *New York Times*, February 17, 2008: http://www.nytimes.com/2008/02/17/opinion/17davis.html?pagewanted=all&_r=0 (last accessed 17 November 2014).

[14]Friedman, *The Law of War*, xx.

[15]Friedman, *The Law of War*, xiii

[16] Solis, *The Law of Armed Conflict*, 187-191

[17] Detter, *The Law of War*, 276-277, 285-288

[18] Detter, *The Law of War*, 148; Solis, *The Law of Armed Conflict*, 187-191.

[19] Detter, *The Law of War*, 148

[20] Richard Shelly Hartigan, *Lieber's Code and the Law of War* (Chicago: Precedent, 1983), 71, (Art 155).

[21] Hartigan, *Lieber's Code,* 55 *(*Art 49 & 50).

[22] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Art 13, 12 August 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31, (hereinafter Geneva I); Geneva Convention for the Amelioration of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Art 13, 12 August 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85, (hereinafter Geneva II); Geneva Convention Relative to the Treatment of Prisoners of War, Art 4, 12 August 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135, (hereinafter Geneva III); A "lawful combatant" is someone who is entitled to fight, who can be targeted and who is authorized POW status if captured.

[23] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 97; 1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land, Annex, Art 1, 18 October 1907, 36 Stat. 2277, 205 Consol. T.S. 277, (hereinafter 1907 Hague IV); Geneva I, Art 13; Geneva II, Art 13; Geneva III, Art 4.

[24] These include: lawful combatants, unlawful combatants/unprivileged belligerents, regular forces, irregular forces, armed forces, prisoners of war, detainees, retainees, civilian internees, members of other militias and members of other volunteer corps, regular armed forces professing allegiance to an unrecognized authority, persons who accompany the armed forces without being members thereof, merchant marine and civilian aircraft crews, levee en masse, militia, volunteer, guerillas, mercenaries, spies, demobilized military personnel and military internees in neutral countries, and civilians who take a direct part in hostilities. *See* Solis, *The Law of Armed Conflict*, 186-238; Detter, *The Law of War,* 135-150.

[25] In fact, the increasing use of private military companies in conflict, employment of remotely piloted aircraft and growth of non-state actors such as Al-Qaeda who employ terrorism, hide among civilians, use civilians as shields and target civilians have all caused increasing tension with the current LOAC paradigm.

[26] *See* P.W. Singer, *Wired For War: The Robotics Revolution And Conflict In The Twenty-First Century* (New York: The Penguin Press 2009).

[27]Clarke and Knake, *Cyber War,* 213-215.

[28] Eric Tegler, *Air Force Flight Simulators May Help Cut Training Costs,* November 11, 2011. http://www.defensemedianetwork.com/stories/virtual-bargain/ (accessed 4 December 2014).

[29] Andrews Tilghman, *In Supersecret Cyberwar Game, Civilian-Sector Techies Pummel Active-Duty Cyberwarriors,* August 4, 2014, http://archive.armytimes.com/article/20140804/NEWS04/308040019/In-supersecret-cyberwar-game-civilian-sector-techies-pummel-active-duty-cyberwarriors (accessed 5 November 2014).

[30]P.W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (Ithaca: Cornell University Press, 2003), 8

[31] Tilghman, *In Supersecret Cyberwar Game, Civilian-Sector Techies Pummel Active-Duty Cyberwarriors.*

[32] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 45-52.

[33] Detter, *The Law of War*, 286-287

[34] Hartigan, *Lieber's Code,* 49 (Art 21 & 22).

[35] *See* 1899 Hague Convention (II) Laws and Customs of War on Land, 29 July 1899, 32 Stat. 1803, Annex, Art. XXIV and XLVI; 1907 Hague Convention (IX) Bombardment by Naval Forces in Time of War, Article I, 18 October 1907, available at http://avalon.law.yale.edu/20th_century/hague09.asp; 1907 Hague IV, Art XXIV and XLVI.

[36] *See* Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 (hereinafter Geneva IV).

[37] Protocol Additional to the Geneva Conventions of August 12, 1949, and relating to the Protection of Victims of International Armed Conflicts, Art 51(2), 12 December 1977, 1125 U.N.T.S. 3, (hereinafter Protocol I).

[38] Protocol I, Art 51(5)(b).

[39] Igor Primoratz, ed, *Civilian Immunity In War* (New York: Oxford University Press, 2007), 2.

[40] Primoratz, ed, *Civilian Immunity In War*, 4

[41] 1899 Hague Convention (IV, 1) Prohibiting the Launching of Projectiles and Explosives from Balloons, 29 July 1899, 32 Stat. 1839.

[42] 1907 Hague Convention (XIV) Prohibiting the Discharge of Projectiles and Explosives from Balloons, 18 October 1907, available at https://www.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=10BB640A9FF13B49C12563CD002D6895&action=openDocument.

[43] 1907 Hague IV, Art 25.

[44] Lee Kennett, *The First Air War: 1914-1918* (New York: Free Press, 1991), 41-62; Tami Davis Biddle, *Rhetoric and Reality in Air Warfare the Evolution of British and American Ideas About Strategic Bombing, 1914-1945* (Princeton, N.J.: Princeton University Press, 2002), 11-68.

[45] Biddle, *Rhetoric and Reality,* 57-68.

[46] Giulio Douhet, *The Command of the Air,* trans. by Dino Ferrari, (Washington, D.C.: Air Force History and Museums Program, 1998), 10 & 57.

[47] Hague Rules of Air Warfare, Art XVIII and XXII, available at http://lawofwar.org/hague_rules_of_air_warfare.htm.

[48] Biddle, *Rhetoric and Reality*, 182-183.

[49] Biddle, *Rhetoric and Reality*, 176-288; R.J. Overy, *The Air War, 1939-1945 (*New York: Stein and Day, 1980), 97-101 & 102-126.

[50] Overy, *The Air War*, 106-108; Biddle 214-232 &261-270.

[51] Overy, *The Air War*, 207-208; Biddle, *Rhetoric and Reality* 277-278.

[52] FOXNEWS.Com. *NSA Director: China can damage US power grid.* November 20, 2014. http://www.foxnews.com/politics/2014/11/20/nsa-director-china-can-damage-us-power-grid/ (accessed December 1, 2014); see also Michael Riley and Jordan Robertson, *Iran-Backed Hackers Target Airports, Carriers: Report,* December 12, 2014. http://www.bloomberg.com/news/2014-12-02/iran-backed-hackers-target-airports-carriers-report.html (accessed December 12, 2014); Reuters. *State-backed Iranian hackers targeted airlines, energy, defense companies, report says.* December 2, 2014. http://www.jpost.com/Middle-East/State-backed-Iranian-hackers-targeted-airlines-energy-defense-companies-report-says-383424 (accessed December 2, 2014).

[53] FOXNEWS.Com. *NSA Director: China can damage US power grid.* November 20, 2014. http://www.foxnews.com/politics/2014/11/20/nsa-director-china-can-damage-us-power-grid/ (accessed December 1, 2014).

Bibliography

1899 Hague Convention (II) Laws and Customs of War on Land, 29 July 1899, 32 Stat. 1803.

1899 Hague Convention (IV, 1) Prohibiting the Launching of Projectiles and Explosives from Balloons, 29 July 1899, 32 Stat. 1839.

1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land, 18 October 1907. 36 Stat. 2277, 205 Consol. T.S. 277.

1907 Hague Convention (IX) Bombardment by Naval Forces in Time of War, 18 October 1907, available at http://avalon.law.yale.edu/20th_century/hague09.asp.

1907 Hague Convention (XIV) Prohibiting the Discharge of Projectiles and Explosives from Balloons, 18 October 1907, available at https://www.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=10BB640A9FF13B49C12563CD002D6895&action=openDocument.

Biddle, Tami Davis. *Rhetoric and Reality in Air Warfare the Evolution of British and American Ideas About Strategic Bombing, 1914-1945.* Princeton, N.J.: Princeton University Press, 2002.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: HarperCollins, 2010

Davis, Morris. "Unforgivable Behavior, Inadmissible Evidence (Op-ed)." *New York Times*, February 17, 2008: http://www.nytimes.com/2008/02/17/opinion/17davis.html?pagewanted=all&_r=0 (last accessed 17 November 2014)

Defense, Department of. *Conduct of the Persian Gulf War: Final Report to Congress.* http://www.dod.mil/pubs/foi/operation_and_plans/PersianGulfWar/404.pdf, April 1992 (accessed 17 November 2014).

Demchak, Chris C., and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly*, Spring 2011: 32-61.

Detter, Ingrid. *The Law of War, second edition.* New York: Cambridge Universty Press, 2000.

FOXNEWS.Com. *NSA Director: China can damage US power grid.* November 20, 2014. http://www.foxnews.com/politics/2014/11/20/nsa-director-china-can-damage-us-power-grid/ (accessed December 1, 2014).

Douhet, Giulio. *The Command of the Air.* Translated by Dino Ferrari. Washington, D.C.: Air Force History and Museums Program, 1998.

Friedman, Leon, ed. *The Law of War: A Documentary History.* Vol. I. II vols. New York: Random House, 1972.

Friedman, SGM (Ret.) Herbert A. *Leaflets of Operation Desert Shield and Desert Storm (continued).* n.d. http://www.psywarrior.com/HerbDStorm2.html (accessed 17 November 2014)

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31.

Geneva Convention for the Amelioration of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 12 August 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85.

Geneva Convention Relative to the Treatment of Prisoners of War, 12 August 1949. 6 U.S.T. 3316, 75 U.N.T.S. 135.

Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

Gerlin, Andrea, and Patrick Peterson. *philly.com.* March 13, 2003. http://articles.philly.com/2003-03-13/news/25474267_1_chemical-warfare-iraqi-soldiers-iraq-kuwait (accessed 17 Novmeber 2014)

Gray, Colin S. *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling.* Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College Press, 2013.

Hague Rules of Air Warfare. Available at http://lawofwar.org/hague_rules_of_air_warfare.htm.

Hartigan, Richard Shelly. *Lieber's Code and the Law of War*. Chicago: Precedent, 1983.

Kennett, Lee. *The First Air War: 1914-1918.* New York: Free Press, 1991.

Nye, Joseph S. Jr. *The Future of Power.* New York: PublicAffairs, 2011.

Overy, R.J. *The Air War, 1939-1945.* New York: Stein and Day, 1980.

Primoratz, Igor, ed. *Civilian Immunity In War.* New York: Oxford University Press, 2007.

Protocol Additional to the Geneva Conventions of August 12, 1949, and relating to the Protection of Victims of International Armed Conflicts, 12 December 1977. 1125 U.N.T.S. 3.

Reuters. *State-backed Iranian hackers targeted airlines, energy, defense companies, report says.* December 2, 2014. http://www.jpost.com/Middle-East/State-backed-Iranian-hackers-targeted-airlines-energy-defense-companies-report-says-383424 (accessed December 2, 2014).

Riley, Michael, and Jordan Robertson. *Iran-Backed Hackers Target Airports, Carriers: Report.* December 12, 2014. http://www.bloomberg.com/news/2014-12-02/iran-backed-hackers-target-airports-carriers-report.html (accessed December 12, 2014).

Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

Singer, P.W. *Corporate Warriors: The Rise of the Privatized Military Industry.* Ithaca: Cornell University Press, 2003.

—. *Wired For War: The Robotics Revolution And Conflict In The Twenty-First Century.* New York: The Penguin Press, 2009.

Solis, Gary D. *The Law of Armed Conflict: International Humanitarian Law in War.* New York: Cambridge University Press, 2010.

Springer, Paul J. *America's Captives: Treatment of POWs from the Revolutionary War to the War on Terror.* Lawrence: University of Kansas Press, 2010

Tegler, Eric. *Air Force Flight Simulators May Help Cut Training Costs.* November 11, 2011. http://www.defensemedianetwork.com/stories/virtual-bargain/ (accessed December 4, 2014).

Tilghman, Andrew. *In Supersecret Cyberwar Game, Civilian-Sector Techies Pummel Active-Duty Cyberwarriors.* August 4, 2014. http://archive.armytimes.com/article/20140804/NEWS04/308040019/In-supersecret-cyberwar-game-civilian-sector-techies-pummel-active-duty-cyberwarriors (accessed 5 November 2014).

von Clausewitz, Carl. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.